AMERICAN FORCES INFORMATION SERVICES

**DESCRIPTION OF THE CONCEPT OF REASONABLE ASSURANCE
AND HOW THE EVALUATION WAS CONDUCTED**

(Tab A)

The system of internal accounting and administrative control of the American Forces Information Services (AFIS), in effect during the fiscal year ending September 30, 2002**,** was evaluated in accordance with the guidance in Office of Management and Budget (OMB) Circular No. A-123 (Revised), "Management Accountability and Control," dated June 21, 1995, as implemented by DoD Directive 5010.38, "Management Control Program," dated August 26, 1996, and DoD Instruction 5010.40, "Management Control Program Procedures," dated August 28, 1996. The OMB guidelines were issued in consultation with the Comptroller General of the United States, as required by the "Federal Managers' Financial Integrity Act of 1982." Included is an evaluation of whether the system of internal accounting and administrative control of the AFIS is in compliance with standards prescribed by the Comptroller General.

The objectives of the system of internal accounting and administrative control of AFIS are to provide reasonable assurance that:

- The obligations and costs are in compliance with applicable laws
- Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation
- Revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of reliable accounting, financial and statistical reports and to maintain accountability over the assets.

The evaluation of management controls extends to every responsibility and activity undertaken by AFIS and is applicable to financial, administrative and operational controls. Furthermore, the concept of reasonable assurance recognizes that (1) the cost of management controls should not exceed the benefits expected to be derived; and (2) the benefits include reducing the risk associated with failing to achieve the stated objectives. Moreover, errors or irregularities may occur and not be detected because of inherent limitations in any system of internal accounting and administrative control, including those limitations resulting from resource constraints, congressional restrictions, and other factors. Finally, projection of any system evaluation to future periods is subject to risk that procedures may be inadequate because of changes in conditions, or that the degree of compliance with procedures may deteriorate. Therefore, this statement of reasonable assurance is provided within the limits of the preceding description.

The evaluation was performed in accordance with the guidelines identified above. The results indicate that the system of internal accounting and administrative control of AFIS in effect during the fiscal year that ended September 30, 2002, taken as a whole, complies with the requirement to provide reasonable assurance that we achieved the above-mentioned objectives. This position on reasonable assurance is within the limits described in the preceding paragraph.

The following describes how the evaluation was conducted:

1.   **Management Control Progress.** The AFIS Management Control Program (MCP) has been institutionalized throughout the agency as well as its field activities. The program ensures all directors, commanders, and senior management officials remain involved in the management control process by making them accountable for the outcome of their respective programs. Annually, AFIS activities reassess programs and functions for which they are responsible for possible inclusion in the MCP. Continual emphasis on management controls and training are the vital links to the program's success.

2.   **Improvements to Program Coverage.** The following actions and events completed during FY2002 continue to improve the AFIS MCP process:

    a. In June 2002 the MCP Coordinator instituted a MCP Monthly Update, which is sent to activity Directors, Commanders, and all management control personnel. It serves as a communication tool for MCP requirements and regularly reinforces the importance of management controls and includes MCP terminology. The letter also informs them of upcoming MCP training events.

    b. The MCP Coordinator completed a draft computer program in Microsoft Excel to automate the MCP process. Information Resource Management (IRM) is translating the program to tailor it to the website. The goal is to fully automate the MCP process, which will facilitate reporting and permit assessable unit managers and MCP Administrators to more efficiently complete, manage, and update required documentation. IRM and the MCP Coordinator are working together to build the requirements to make this a successful program.

    c. A draft of the revised MCP Handbook will be completed in October 2002. The revision will permit users to navigate and search for information quicker and will emphasize the importance of management control by effectively linking them with the organization's goals and objectives.

3.   **Problems Encountered in Implementing the Program.** None

4.   **Other program considered.** None

5.   **Deviations from the process as outlined in the OMB guidelines.** None

6.   **Special concerns addressed in reports by the DoD IG regarding the management control process, program needs, or problems.** None

7.   **Methods, mechanisms, or techniques employed in the discovery or execution phases of the program***:*

    a.   **A weakness tracking system** is incorporated throughout the AFIS MCP that identifies both material and non-material weaknesses and the milestones for correction. MCP Administrators at each field activity level maintain this tracking system as well as the overall status through the submission of quarterly reports. There were no material weaknesses reported this year.

b. **Significant component IG findings.** None

c. **Reports of Internal Reviews & Inspections.** Each fiscal year AFIS activities plan and conduct risk assessments (RAs), management control reviews (MCRs), and corrective action reviews (CARs). These reviews and assessments are based on a 5-year plan that ensures each activity analyzes each assessable unit according to its risk level. In addition to the external reviews, AFIS and its field activities conducted 45 risk assessments, 16 management control reviews, and 8 alternate management control reviews this fiscal year.

The following reviews / inspections took place at AFIS:

December 2001-the Logistics Branch completed the Tri-Annual Personal Property and Equipment (PP&E) Inventory. The accuracy rating of the inventory was 99.992%. Inadequate records retention requirements of our file-plan resulted in minor discrepancies. No material weaknesses were discovered. We continue to perform our annual 100% inventories (10% monthly) to ensure the accuracy of the DPAS records.

February 2002-The Federal Protective Service (FPS) completed a Building Security Assessment for 601 North Fairfax Street. The purpose was to evaluate and offer recommendations to improve the security posture of the facility. The Physical Security Specialist reported that our security measures exceeded those required of a Level II facility.

February 2002- the SmartPay card-approving official completed an internal review of all purchase card accounts. It was completed using the Defense Contracting Command-Washington (DCC-W) checklist taken from the "DCC-W User's Guide for Cardholders and Billing Officials to the SmartPay Purchase Card Program." There were no material weaknesses.

February 2002-members from the DCC-W audit team inspected our credit card program. They randomly reviewed numerous purchases for appropriate documentation accuracy, completeness and regulatory compliance. There were no material weaknesses.

June 2002 - Independent Budget and Best Practices Review from KPMG Consulting, LLC (Appendix B-4).

July 2002-Abdul Bangura, an auditor for the Army Audit Agency, completed a SmartPay review of a purchase, which was randomly selected by a new Army software program to monitor purchases. We met or exceeded all documentation and regulatory requirements for the purchase.

Kastle Card Audits. We conduct monthly Kastle Card audits to ensure complete card accountability. These cards enable employees to enter the building. An updated assignment list is downloaded from Kastle, and then the on-hand stock is checked against the list. Access into the Kastle system will immediately be suspended, when a card is identified as missing or not accounted for.

Security Guard Procedures. The GSA Security Guard Inspector visits the security guard desk weekly to ensure that guards and employees adhere to the security procedures outlined in the post orders. The inspector observes the guard and employees entering to make sure that ID cards are clearly in sight, visitors have shown a valid ID before signing the visitors' log, packages are handled in accordance with the post orders, and equipment removed from the 3rd floor is either logged into the Equipment Movement Log or the employee has an official Property Pass.

The transformation of DINFOS resulted in a new section called Standards and Evaluations (SES). DINFOS established the SES to review all courses in a 100% instructional system development audit. As a result, seven Assessable Units (AUs) fall under the SES and no longer fall under the MCP. All scheduled internal inspections for last year were rescheduled for the next fiscal year. Eleven DINFOS personnel received MCP training this Fiscal Year. In May 2002, the OASD(PA)/AFIS MCP Coordinator conducted an AMCR for the property accountability to determine whether control techniques are working properly. It is similar to an MCR. However, it is not shown on the 5-year plan because it is not a scheduled event.

DVIC conducted MCRs in Customer Service and Time & Attendance. In May 2002, the OASD(PA)/AFIS MCP Coordinator conducted an AMCR for the property accountability. DVIC has 100% trained MCP personnel.

JVISDA conducted an MCR in Information Security. JVISDA has 100% trained MCP personnel.

Collectively, Stars and Stripes (S&S) completed six MCRs for Risk Management Program (RIMP) Insurance, safety, property book, performance appraisals, production quality control, and sales activities. S&S also conducted 35 vulnerability assessments and conducted inspections of cash management, cashier cages/safes, general ledger procedures, accounts payable activities, and management of appropriated fund processes. Four S&S personnel received MCP training this fiscal year.

T-ASA conducted MCRs and Risk Assessments for Logistics, Warehouse Operations and Warehouse Physical Security and three Risk Assessments for Physical Security, Information Resource Management, and Budget and Finance. T-ASA also assessed the management controls of the Accounts Payable – Payment Certification Process. Defense Logistics Agency (DLA) reviewed Procurement Management for T-ASA Contracting offices in January 2002 to include the overall integrity of the procurement system, business practices, pre and post award processes, contracting workforce development, and business management. T-ASA's Contracting procurement process was commended due to their comprehensive oversight and review program. In May 2002, the OASD(PA)/AFIS MCP Coordinator conducted an AMCR for the property accountability.

d. **Outstanding DoD IG reports or reviews.** None

e. **MCP Training.** Fifteen AFIS employees received formal Integrity Act (FMFIA) compliance training. An instructor from Management Concepts, located in Vienna, Virginia, trained AU managers and supervisors to ensure proper program emphasis and standardization of

information. The 3-day session covered the Integrity Act as well as comprehensive guidance and instruction for implementing MCP program requirements so that managers can better fulfill their MCP duties and responsibilities. Training is and will continue to be an ongoing process and a priority to ensure all employees understand the MCP process and its importance.

        f.   **MCP Performance Standards.** MCP requirements are addressed as a separate element in the performance appraisals process of all AU managers, program managers, and supervisors having MCP responsibility.

        g.   **GAO Reports & Reviews.** Both the Army Audit Agency and Defense Contracting Agency reviewed the IMPAC Card account. No written report is expected from the Army Audit Agency. The Defense Contracting Agency stated our records are well organized and in good condition.

        h.   **Review of Office of the Secretary of Defense (OSD) Functional Proponent Proposals (e.g., systemic weaknesses).** Not applicable.

        i.   **Information Technology (IT) initiatives.** A summary of the recent developments in each of the Assessable Units is shown below:

        Planning, Budgeting, Procurement and Asset Management. During the first quarter, IRM used the newly developed Budget Management System (BMS) in conjunction with internal IRM budget documentation. This system ensures that IRM continues to operate within funding levels designated for IT procurements and that funds are properly managed. The BMS, which provides a central collection point for budget data for the HQ directorates and field sites, increased the management control of the IT budget process by eliminating the risk of errors when multiple systems are used to collect data.

        IRM conducted reviews of the IT asset management processes, controls, and safeguards to ensure they are suitable to protect from fraud, waste and mismanagement. We updated inventory procedures as a collaborative effort between IRM and the property book holder to improve controls and safeguards over IT assets. IRM continues to use hand receipts to assign responsibility and accountability of IT assets within the organization and have proven to be an invaluable tool.

        Applications Life Cycle. IRM successfully implemented the system architecture researched during FY01. This architecture supported the development of critical applications for our organization to include an automated budget tracking system, web content management system, budget submission system and smaller systems to automate business processes. The application development efforts reduced costs and increased productivity. Future systems will focus on supporting the integration of all organizational elements of OASD(PA). The integration highlighted changes in business processes that these new systems will address.

        Operations, Network Security, Equipment and Software Management. We track IT assets from acquisition through retirement using a local IRM Asset Management system. Washington Headquarters Service (WHS) conducts inventories to validate the accuracy and scope of reported IT assets. WHS performed an annual audit of all IT financial records, contract

files, and record-keeping procedures and reported that we meet WHS IT financial management and record-keeping requirements.

       j.   **MCP References in Directives, Regulations, and Other Guidance.** All activities continue to follow OP 20 and the MCP Handbook. A revised draft of the handbook is complete and will replace the current version already on the website. These documents incorporate the intent and requirements of the FMFIA while providing clear, succinct guidance.

       k.   **Congressional reviews and hearings.** Not applicable.

       l.   **Command or Other Subordinate Organization "Letters of Assurance."** Annually, field activity directors and program directors submit a statement of assurance to the director of Administration and Management stating whether they can provide reasonable assurance that the management control systems under their cognizance are in place and working in accordance with applicable guidance. A summary of their contributions is in paragraph c.

       m.   **Productivity statistics.** Not applicable.

       n.   **Defense Regional Interservice Support Studies**. Not applicable.

       o.   **Management reviews in other functional areas (e.g., procurement; command, control, communications and intelligence; financial; or environmental).** Not applicable.

       p.   **Quality Assurance reviews.** Not applicable.

q.   **"Hot Line" reports.** On August 22, 2002 AFIS received a DISA-IG correspondence [Control Number: PAO000393-2002] regarding a possible presence of an active Internet mail relay on the T-ASA network. The IRM office contacted the T-ASA IR to determine if the active Internet mail relay existed. The mail relay occurred due to a missing operating system patch. The patch was then applied and the relay was eliminated. Both T-ASA and IRM conducted tests on the system and verified that the patch successfully removed the Internet mail relay.

Office of the Secretary of Defense (OSD) Systemic Weakness Disclosure

No systemic weaknesses were identified.

AMERICAN FORCES INFORMATION SERVICES

MANAGEMENT CONTROL PROGRAM AND RELATED ACOMPLISHMENTS

(Tab B-4)

1. Internal Assessment of the Budget, Contract, and Property Accountability Processes of the field activities.

    Description: An ad hoc team consisting of two military finance officers and two external contractors (one independent contractor and former Chief of Contracting at AFRTS-BC, and one consultant from KPMG Consulting, LLC) reviewed the budgeting and contracting processes.

    Purpose: The purpose and scope of the review was to "…ensure proper management of fiscal resources required to sustain all AFIS missions and functions…" as well as Best Practices assessment employed by AFIS activities.

    Conclusion: The review showed that;

       a. There is no appearance of intentional or inadvertent violation of statute in the conduct of business operations within domains of budgeting, contracting, and property accountability.

       b. Assurance against waste, fraud, and mismanagement is adequate given adherence to proper contracting, budgeting, and property book procedures.

2. KPMG Consulting's, LLC external assessment of the field activity budget processes and Best Practices.

    Overview: KPMG was contracted to perform an independent assessment of the budget processes.

    Purpose: The purpose was to conduct an independent review and identify deficiencies and Best Practices by visiting the sites, reviewing policies and standard operating procedures and evaluating the budget management system.

    Conclusion: "In general, KPMG Consulting found that the budget processes at AFIS and the organizational elements, when utilized properly, do provide adequate protection against fraud, waste and mismanagement of Agency resources. The processes, though not standardized, allow AFIS to adhere to all Office of the Secretary of Defense, Comptroller (OSD(C)) budget submission requirements in an accurate and timely manner."

3. IMPAC Card Review.

Overview: Members from the DCC-W audit team conducted an inspection of our credit
card program.

Purpose: The purpose of the review was to verify documentation accuracy, completeness and regulatory compliance.

Conclusion: All minor discrepancies were subsequently corrected and no material weaknesses were identified.

4. AFRTS-BC/DVIC Building Security Enhancement

Description: The building security camera surveillance focused on strategic points of entry to the facility was inadequate to provide for maximum-security coverage.

Accomplishments: To improve security coverage, additional cameras were mounted at the strategic points of entry increasing the surveillance of vehicles and pedestrians entering the facility. This addition reduced the contract staff by one person without compromising the coverage.

5. AFRTS-BC/DVIC System Management Server

Description: The Information Technology (AFRTS-BC-IT) Division needed to remotely access network computer systems for troubleshooting, software distributions and asset management.

Accomplishments: AFRTS-BC-IT purchased Microsoft Systems Management Server (SMS) to accomplish these required tasks. SMS allows us to control any computer on our network and to troubleshoot from the help-desk office. This enables us to fix problems quicker by eliminating the need to physically visit each trouble call. It gives us the ability to remotely load software and security patches to multiple computers simultaneously without having to physically load these patches and updates. It also shows which computers need critical system and security updates, it allows us to reconcile deployed software purchases or those currently in use, and it also identifies software that has been loaded and not yet purchased.